CONTRATO DE ASOCIACIÓN PARA EL DESARROLLO DE UNA APLICACIÓN

Fecha: 01/06/2024

Partes:

Este contrato se celebra entre las siguientes personas, todas mayores de edad y con domicilio en Córdoba, en adelante denominados colectivamente como "los Desarrolladores".

Objeto:

Los Desarrolladores acuerdan asociarse para el desarrollo de una aplicación destinada a facilitar las transacciones entre inversores (personas físicas, empresas o instituciones) y otros inversores dentro del Mercado de Valores de Buenos Aires (Merval).

Distribución de Beneficios:

Se acuerda que cualquier beneficio derivado del desarrollo y explotación de la aplicación será distribuido equitativamente entre los Desarrolladores, conforme al siguiente criterio:

Cada Desarrollador recibirá un 16.67% (1/6) de los beneficios totales.

Responsabilidades:

Cada Desarrollador se compromete a contribuir con sus habilidades y conocimientos al desarrollo de la aplicación según sea necesario, y a trabajar de manera colaborativa con los demás Desarrolladores para lograr los objetivos del proyecto.

Propiedad Intelectual:

Se acuerda que la propiedad intelectual resultante del desarrollo de la aplicación será propiedad conjunta de todos los Desarrolladores. Cualquier explotación comercial de la misma requerirá el consentimiento unánime de todos los Desarrolladores.

Duración:

Este contrato entrará en vigor en la fecha de su firma y continuará hasta la finalización del desarrollo de la aplicación, a menos que sea terminado anticipadamente por mutuo acuerdo de todos los Desarrolladores.

Describir quiénes y ante quien deben matricularse a nivel provincial para ejercer la Profesión según Ley 7642 del Consejo profesional de Ciencias Informáticas de la provincia de Córdoba

En todo el territorio de la Provincia de Córdoba queda sujeto a Io que prescribe la presente ley y a las disposiciones reglamentarias que se dicten, el ejercicio de las profesiones en Ciencias Informáticas. A tal fin es obligatoria la inscripción de la matrícula que le otorgue el Consejo Profesional de Ciencias Informáticas de la Provincia de Córdoba.

Describir que requerimientos deben cumplir el código programado y las bases de datos según la legislación vigente

Cumplir con la Ley 25326 de protección de datos personales, asegurando que los mismos sean tratados de manera segura y confidencial.
Utilizar técnicas de encriptación para proteger datos sensibles durante la transmisión y almacenamiento.
Implementar medidas técnicas y organizativas para asegurar la protección de los datos contra accesos no autorizados, alteraciones y destrucción.
Cumplir con estándares de calidad reconocidos para la calidad del software como la ISO IEC 25000.
Realizar pruebas de funcionalidad, rendimiento, seguridad y usabilidad del software.
Mantener una documentación completa y actualizada del código fuente y especificaciones técnicas.
Asegurar que el código desarrollado este protegido bajo la legislación de derechos de autor, y no infrinja derechos de autor de terceros.
Implementar controles de acceso adecuados para garantizar que solo personal autorizado pueda acceder a los datos sensibles.
Realizar auditorías y monitoreos para detectar y responder a posibles incidentes de seguridad.
Implementar políticas de respaldo y recuperación de datos para asegurar la disponibilidad e integridad de la información.
Mantener registros detallados de todas las actividades realizadas sobre la base de datos, incluyendo acceso, modificación y eliminación de datos.

Enumerar los pasos para que ARGBroker sea parte del Registro Nacional de software.

Importante: La obra debe estar publicada previo al inicio del trámite.
Documentación necesaria para iniciar el trámite:

- Comprobante de pago del trámite
- Comprobante de pago de la tasa
- Copia de la obra completa
- Datos de la obra a declarar:
    - Autor y/o coordinador (si fuera obra colectiva).
    - Breve descripción de la obra y calificación del software.
    - Identificación del titular.
- Datos a proporcionar de los autores:
    - N° de CUIL/CUIT. En caso de ser extranjero: CDI/Pasaporte

- Ingresa a TAD-Inscripción de obra publicada – Software e inicia el trámite.

Si un integrante del grupo no realiza el trámite de matriculación, que pena le corresponde a nivel provincial.

El ejercicio de las profesiones en Ciencias informáticas por personas no inscriptas en el consejo con su correspondiente matrícula, será penado por multas en dinero que oscilarán entre diez (10) y quinientas (500) veces el valor del derecho a la Inscripción a la matrícula.

Si el código es replicado, describir como la Ley de Propiedad Intelectual puede salvaguardar a ARGBroker

Sanciones ante violaciones: Artículo 72 Ley 11.723
Prisión de 1 mes a 6 años
Para quien defraude derechos de propiedad intelectual (edite, venda, reproduzca o falsifique obras intelectuales sin autorización).
Además, el ilícito es resarcible civilmente mediante una acción de daños y perjuicios.

Si un integrante del grupo divulga los datos de la base de datos interna, describir como legalmente deberían accionar los demás.

En el supuesto de que algún integrante del grupo divulgara datos de la base de datos interna, se realizará por parte de los demás integrantes de la asociación la denuncia correspondiente tipificada en el Art. 157 bis del código penal:
"Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley."

Si otro integrante del grupo reutiliza el código para fines personales, describir como legalmente deberían accionar los demás según la Legislación de la Provincia de Córdoba y el Código Penal Argentino.

En el supuesto de que un integrante reutilizara el código para fines personales, se realizara la correspondiente denuncia ante el Consejo Profesional de Ciencias Informáticas de la Provincia de Córdoba aportando por escrito: El nombre o nombres y datos del denunciante, la relación del hecho, la indicación del autor y partícipes, las pruebas de las que se dispongan, la constitución de un domicilio y la firma o firmas de denunciantes.
Asimismo, se realizará la correspondiente denuncia tipificada en el Código Penal:
Art. 172: "Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.
Art. 153: "Será reprimido con prisión de quince (15) días a seis (6) meses el que, sin orden de autoridad competente, abriere, accediere indebidamente, divulgare o

utilizare en perjuicio de otro, una comunicación electrónica, un archivo, un registro, una carta, un pliego cerrado, un despacho telegráfico, telefónico, o de otra naturaleza que no le esté dirigido, aunque no se haya causado daño."

Si otro integrante del grupo reutiliza el código para fines personales a nivel internacional, describir qué instrumento legal respalda a ARGBroker.

En el supuesto que un integrante de la empresa ARGBroker, reutilizara el código para fines personales a nivel internacional, se realizara la correspondiente denuncia ante las autoridades locales basándose en el Convenio de Budapest sobre Ciberdelincuencia, indicando que se ha cometido una infracción de propiedad intelectual a nivel internacional:
Art. 10: Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.
Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delitos en su derecho interno la infracción intencional, a escala comercial, de los derechos de autor y derechos conexos establecidos por la legislación de esa Parte, de conformidad con las obligaciones que le incumben en virtud del Convenio de Berna para la Protección de las Obras Literarias y Artísticas, el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio y el Tratado de la OMPI sobre Derechos de Autor, salvo cuando el derecho se realice conforme a los acuerdos de licencia u otras autorizaciones previstas por la ley o la autoridad competente.
Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delitos en su derecho interno la infracción intencional, a escala comercial, de los derechos afines a los derechos de autor establecidos por la legislación de esa Parte, de conformidad con las obligaciones que le incumben en virtud del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, salvo cuando el derecho se realice conforme a los acuerdos de licencia u otras autorizaciones previstas por la ley o la autoridad competente.

Si la base de datos es adulterada de manera externa, a nivel nacional, describir qué instrumento legal respalda a ARGBroker.

En caso de que la base de datos sea alterada de manera externa se realizaran las correspondientes acciones legales basándose en la Ley 26388 del Código Penal Argentino:
ARTICULO 10. — Incorporase como segundo párrafo del artículo 183 del Código Penal, el siguiente:
En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.
ARTICULO 5º — Incorporase como artículo 153 bis del Código Penal, el siguiente:
Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

Si los datos de la base de datos son adulterados de manera externa, a nivel internacional, describir qué instrumento legal respalda a ARGBroker.

En el supuesto que los datos de la base de datos fueran adulterados de manera externa se procederá a la correspondiente denuncia ante las autoridades locales basándose en el Convenio de Budapest en base a los siguientes artículos:
Art. 2: Acceso ilícito
Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delitos en su derecho interno, cuando se cometan intencionalmente, la acción de acceder de manera ilícita a todo o parte de un sistema informático.
Art. 3 Interceptación ilícita
Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delitos en su derecho interno, cuando se cometan intencionalmente, la acción de interceptar sin derecho, mediante medios técnicos, transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema informático, incluidas las emisiones electromagnéticas procedentes de un sistema informático que transporte esos datos.
Art. 4 Ataques a la integridad de los datos
Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delitos en su derecho interno, cuando se cometan intencionalmente y sin derecho, la alteración, destrucción, deterioro o supresión de datos informáticos.
Artículo 6: Abuso de dispositivos
Texto: Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delitos en su derecho interno:
La producción, venta, adquisición para uso, importación, distribución u otro modo de poner a disposición: a. Un dispositivo, incluido un programa informático, concebido o adaptado principalmente para permitir la comisión de cualquiera de los delitos establecidos de conformidad con los artículos 2 a 5; b. Una contraseña informática, un código de acceso o datos similares que permitan acceder a todo o parte de un sistema informático, con la intención de permitir que otro cometa cualquiera de los delitos establecidos de conformidad con los artículos 2 a 5.
La posesión de un dispositivo, una contraseña informática, un código de acceso o datos similares a los mencionados en el apartado 1 del presente artículo, con la intención de utilizarlos para cometer cualquiera de los delitos establecidos de conformidad con los artículos 2 a 5.

Cuando los programadores de ARGBroker incurren en una negligencia, a que instrumento legal se acude y quien.

La persona afectada puede acudir, dependiendo la gravedad, al Consejo Profesional de Ciencias Informáticas de la Provincia de Córdoba, o ampararse en alguna de las leyes establecidas por el código penal, protección de datos personales, etc.

Cómo ARGBroker debe implementar seguridad según la Ley de Protección de Datos Personales.

ARTICULO 9° — (Seguridad de los datos).
1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no,

de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.
ARTICULO 10. — (Deber de confidencialidad).
1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.
2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Si el cliente decide reemplazar a ARGBroker por otro proveedor, describir cómo se debe actuar de manera ética ante el cliente y los colegas.

Ante el Cliente:
Aceptar la decisión del cliente con profesionalismo y sin resentimientos.
Si es posible, entender las razones detrás del cambio para mejorar en el futuro.
Informar al equipo interno sobre la decisión del cliente y los pasos a seguir.
Desarrollar un plan detallado para la transición de los servicios al nuevo proveedor.
Asegurarse de que todos los datos necesarios se transfieran de manera segura y completa.
Proporcionar toda la documentación relevante para facilitar la transición.
Seguir proporcionando los servicios acordados hasta el final del contrato.
Asegurar una transición suave para que el cliente no sufra interrupciones en el servicio.
Pedir retroalimentación sobre el servicio prestado y la razón del cambio para identificar áreas de mejora.
Hacia los colegas:
Comunicar la decisión del cliente de manera abierta y transparente.
Reducir la posibilidad de rumores al ser claro y directo sobre la situación.
Trabajar en equipo para asegurar que la transición se realice de manera efectiva y profesional.
Motivarlos a ver esto como una oportunidad para aprender y mejorar.
Analizar internamente las razones del cambio y discutir cómo se pueden implementar mejoras.
No hablar negativamente del cliente ante otros colegas o en entornos profesionales.
Promover una cultura de respeto y profesionalismo, independientemente de las circunstancias.
Celebrar los logros alcanzados con el cliente y usarlos como motivación para futuros proyectos.

Si un usuario denuncia a ARGBroker por divulgación de sus datos personales, a que legislación recurrió el mismo y como ARGBroker puede respaldarse jurídicamente

Si un usuario denuncia a ARGBroker por divulgación de sus datos personales, el usuario está recurriendo a la Ley de Protección de Datos Personales de Argentina, conocida como Ley 25.326. Esta ley establece los derechos de los titulares de datos personales y las obligaciones de los responsables del tratamiento de dichos datos para proteger la privacidad y la integridad de la información personal.

Cómo ARGBroker puede respaldarse jurídicamente

Asegurar que ARGBroker tenga una política de privacidad clara, accesible y comprensible que explique cómo se recopilan, utilizan, almacenan y protegen los datos personales.

Demostrar que los datos personales fueron recopilados con el consentimiento explícito, informado y previo del usuario.

Tener contratos y términos de servicio bien redactados que expliquen las prácticas de manejo de datos y aseguren que los usuarios han aceptado estos términos.

Probar que se han implementado medidas técnicas y organizativas adecuadas para proteger los datos personales contra acceso no autorizado, pérdida, destrucción, uso indebido, o divulgación.

Documentar y demostrar que el acceso a los datos personales está restringido solo al personal autorizado.

Realizar y presentar auditorías de seguridad periódicas para demostrar la continua vigilancia y mejora de las medidas de seguridad.

Contar con procedimientos para notificar rápidamente a la Agencia de Acceso a la Información Pública y a los usuarios afectados en caso de una violación de seguridad de los datos.

Proporcionar evidencia de que se han respetado y facilitado los derechos de los usuarios de acceder, rectificar y cancelar sus datos personales cuando lo soliciten.

Tener procedimientos documentados para responder rápidamente a las solicitudes de los usuarios relacionadas con sus derechos sobre sus datos personales.

Demostrar que todo el personal ha recibido formación adecuada y continua sobre la protección de datos personales y las políticas de la empresa.

Mantener toda la documentación legal que respalde el cumplimiento de la ley, incluyendo registros de consentimiento, políticas de privacidad, y evidencia de medidas de seguridad implementadas.